DATA PROCESSING SYSTEMS

ጎ	ABSTRACT
<u>_</u>	

1

3	Detection of an attack on a data processing system. An
4	example method comprising, in the data processing system:
5	providing an initial secret; binding the initial secret to
6	data indicative of an initial state of the system via a
7	cryptographic function; recording state changing
8	administrative actions performed on the system in a log;
9	prior to performing each state changing administrative
10	action, generating a new secret by performing the
l 1	cryptographic function on a combination of data indicative
12	of the administrative action and the previous secret, and
13	erasing the previous secret; evolving the initial secret
14	based on the log to produce an evolved secret; comparing the
15	evolved secret with the new secret; determining that the
16	system is uncorrupted if the comparison indicates a match
17	between the evolved secret and the new secret; and,
18	determining that the system in corrupted if the comparison
19	indicate a mismatch between the evolved secret and the new
20	secret.

Docket Number: CH920020047US1 27